Chapter 15:   Installing Fermi Kerberos on a Linux System

In this chapter we discuss installing the Fermilab **kerberos** product and Kerberized **ssh** on a RedHat Linux or Fermi RedHat Linux machine via **RPM**[1], and point you to installation instructions. These products are also available as **UPS** products from *fnkits.fnal.gov.*

For your reference, the Fermilab Linux pages are online at `http://www-oss.fnal.gov/projects/fermilinux/`. Be aware that FermiLinux comes with kerberized network services turned off.

15.1 Before You Install Kerberos

15.1.1 Choose your Installation Method

Both the RPM and UPS/UPD installation frameworks are available for Kerberos on Linux machines. Both methods perform the installation of all the Fermilab Kerberos tools and configuration settings and satisfy the Fermilab policy requirements, but RPM is the recommended method.

The RPM install leaves the systems in a PAM-aware configuration such that more of the normal RedHat tools function as expected. We recommend this installation for people using either the stock RedHat or the FRHL configuration. The major advantages of this method are seen to be:

> 1) the potential for automatic updates via the AutoRPM service
>
> 2) the closer alignment with stock RH product management tools
>
> 3) increased ease of use for non-FNAL/non-UPS/UPD configurations

We recommend the UPS/UPD method only for people running servers in the UPS framework.

15.1.2 Differences between the UPS/UPD and RPM Ker-

1. We describe installation for fully-strengthened mode only; due to details of the PAM configuration, the mixed-mode installation would violate Fermilab policy.

beros Products

Configuration

The UPS product configuration uses a perl script, the RPMs use bash scripts. For the most part all the RPM install scripts immitate what is done during the UPS product install. The perl product in UPS can sometimes interfere with the perl native to RHL and cause problems.

The UPS Kerberos product is designed to be installed interactively, whereas an RPM is designed to be installed without any interaction, except for the `makehostkeys` script which must be run manually after everything else is installed. The `makehostkeys` script creates the `/etc/krb5.keytab` file, which allows Kerberized logins to a machine.

The `/etc/krb.conf` configuration file for RPM currently differs from that for the UPD/UPS Kerberos product, in order to work with the PAMs.

Login Program

The RPM Kerberos login program (`krb5-fermi-login`) authenticates users at the login prompt with their Kerberos passwords, but may prohibit users from starting X windows. We plan to eventually replace this program with PAM modules. For now, we recommend that you install this login program and try it out with the rest of the RPM Kerberos package. If you have any problems starting X windows, just remove the login RPM.

15.1.3 Follow Same Pre-install Steps as for UNIX

Obtain a Kerberos principal	See section 3.1.2 *Requesting a Principal.*
Create an account on the machine that matches your principal	See section 14.1.2 *Create an Account that Matches your Principal.*
Determine if you need to allow incoming Kerberos connections and/or FTP access. If so get a fixed IP and obtain host and service principals and passwords.	See section 14.1.6 *Do you Need to Allow Incoming Kerberos Connections?.*
Synchronize your machine with a time server	See section 14.1.7 *Synchronize your Machine with Time Server.*

15.1.4 Create a Local Account

For individuals who administer their own desktops, we recommend that you create two accounts: one that matches your principal and from which you will authenticate to Kerberos (listed in section 15.1.3 *Follow Same Pre-install Steps as for UNIX*), and a local account for which the username does not match your principal and which will not be used for Kerberos-related activity. The local account is really just a convenience so that you can always access your machine, even if the network is down or you are not able to access the Kerberos servers. For a local account, its password must adhere to the following three conditions:

- the password hash must be stored locally (no NIS, LDAP, etc.),
- the password cannot be used for network access (restrict to `securetty`)
- the password cannot contain your Kerberos password and cannot be not similar to it

15.1.5 PAM and Passwords for Desktop Environment Applications

A number of applications on Linux (e.g., screensaver, graphical login, console login) use local authentication checks via the PAM libraries.

There is no easy way to use kerberos with PAM in the 6.x enviroment. Thus the passwords that you use in your desktop enviroment applications must be different from your Kerberos password.

For FRHL 7.1.1 or RedHat 7.1, the installation instructions include steps to make all of the desktop enviroment applications use your Kerberos password. If you want these passwords to be the same as they were before, skip the last couple of steps as noted on the instructions (below). An alternative to configuring PAM is to allow only text-based logins and use the FNAL `login.krb5`.

The PAM for RedHat 7.3 and 8.0 (also used in FRHL 7.3.1) has been improved, and your Kerberos password is used by default for all local authentication.

15.1.6 SSH and OpenSSH

If you are running Scientific Linux Fermi, the Fermi OpenSSH rpms should be already installed. If you are running some other distribution, look for something compatable at `ftp://linux.fnal.gov/linux/contrib/openssh/`.

15.2 Kerberos and OpenSSH RPM Installation

Log in as *root* to perform the installations. Follow the instructions at `http://www-oss.fnal.gov/projects/fermilinux/common/kerberos.html` for the OS version you have. Descriptions of the Fermi Kerberos and ssh RPMs can also be found on that page.

For more information, or to do a custom install, see the various README files that come with the Fermi ssh and Kerberos products (go to `ftp://ftp.fnal.gov:8021/products/kerberos/,` choose a version, and continue down the branch to find the files).